

# Encryption at Rest

## Cloud Hosting Services

## Encryption at Rest

GeoPlatform securely manages your data in the cloud using the industry standard AES-256 (Advanced Encryption Standard) algorithm for the encryption of data in EBS (Amazon Elastic Block Store), backups & snapshots, S3 (Amazon Simple Storage Service), and AMIs (Amazon Machine Image) automatically at time of launch per the guidelines of STIG (Security Technical Implementation Guide). The “Encryptotron” tool automatically encrypts volumes if they are unencrypted to ensure data security.



### STIG'd Operating Systems

- RedHat 7
- CentOS 7
- Oracle Linux 7
- Windows Server 2012
- Windows Server 2016



### Policies

- All new S3 buckets use AES-256 server side keys by default
- IAM Users will only be able to launch images that are encrypted
- IAM Users will only be able to create S3 buckets with AES-256 enabled on the server side
- IAM Users can only launch encrypted RDS (Amazon Relational Database)



### Snapshots

- Backed up daily and saved for a week
- Backed up weekly and saved for a month
- Backed up monthly and saved indefinitely



### Encryptotron

- Backs up instances
- Stops instances
- Creates a snapshot of all volumes on the instance
- Copies all snapshots and applies the encryption during copy
- Creates a new encrypted volume from the encrypted snapshot
- Reattaches the volume to the instance
- Relaunches the instance
- Cleans up the explosion of snapshots and volumes